Policy Number: P-104A
Amended Date: January 27February 2, 2004
Revision: 4Effective Date: February 6, 2004

STATE OF COLORADO

Information Technology Resource Management Standard

Colorado Data Destruction Policy
and
Computer/Other Electronic Media
End-of-Life Policy

Governor's Office of Innovation and Technology

Preface

Publication Designation

POLICY NUMBER: P-104A

Subject

Colorado Data Destruction and Computer/Other Media End-of-Life

Effective Date

Immediately upon approval and promulgating; no later than July 1, 2004

Supersedes

No prior Standards or Policies

Scheduled Review

One (1) year from effective date.

Authority

Governor's Office of Innovation and Technology (OIT)
COLORADO REVISED STATUTES 24-37.5-101-106

Colorado Information Security Task Force (CISTF)

Scope

This standard is applicable to all State agencies, their field operations, and institutions of higher education (collectively referred to as "Agency") that surplus, transfer, trade-in, otherwise dispose of, or replace the computer hard drives and electronic media resources in Colorado. This standard also applies to equipment owned or leased by the agency. The heads of State agencies, the heads of their field offices, and the heads of institutions of higher education are responsible for compliance with this standard. This standard is offered as guidance only to local government entities.

Purpose

1. To define the minimum requirements for the removal of Colorado data from an agency's computer hard drives and electronic media resources prior to its being surplused, transferred, traded-in, disposed of, or the hard drive is replaced.
2. To prevent unauthorized use or misuse of state information, and promote the privacy and security of sensitive and/or confidential information resources within Colorado.
3. To foster state agency compliance with federal regulations dealing with the confidentiality of personally identifiable information. Included are regulations such as the Health Insurance Portability and Accountability Act (HIPPA), the Gramm-Leach-Bliley Act (aka, Financial Services Modernization Act), and the Family Educational Rights and Privacy Act.
4. To prevent hazardous waste from the disposal of computers and other electronic media.

Objectives

1. Define and promulgate the minimum requirements for the removal of Colorado data from an agency's computers and electronic media resources prior to its being surplused, transferred, traded-in, disposed of, or replaced.
2. Define a process to certify an agency's removal of Colorado data from its computers other electronic media resources.
3. Define a process to audit the removal of Colorado data from an agency's computer hard drives and other electronic media resources.

General Responsibilities

This policy/standard is issued under the authority of the State Chief Technology Officer in accordance with Colorado Revised Statute (C.R.S. 24-37.5-106 and under the guidance of the Commission on Information Management in accordance with the C.R.S. 24-37.5-201.

All State Agencies

All State Agencies are responsible for complying with Colorado Information Security Task Force (CISTF) policies and standards and considering CISTF guidelines issued by the Chief Technology Officer.

Related OIT Policies, Standards, and Guidelines

OIT Policy: IT Security Policy P-104
Information Technology Standards

CISTF Policy: Information Security Standard

Definitions

Data Destruction: the process of removing sensitive and/or confidential programs or data files on computers or electronic media in a manner that gives assurance that the information cannot be recovered.

Physical Destruction – to disintegrate, incinerate, pulverize, shred or melt the hard drives or other electronic media.

Total Destruction of Information Technology Equipment: - The reduction of ALL components of equipment and ALL associated electromagnetic media to its original elemental form.

Operable hard drives – hard drives that have the ability to work (be operable).

Inoperable hard drives – hard drives that do not have the ability to work (be operable).

RECYCLE – AFTER PHYSICAL DESTRUCTION, RECYCLING THE RAW PLASTICS, METALS, GLASS FOR RE-USE.

Table of Contents

Background

The surplusing, transfer, trade-in, disposal of computers, or replacement of electronic storage media, and computer software can create information security risks for the agency. This also includes equipment reassigned, or released, or no longer in use in the agency. These risks are related to potential violation of software license agreements, unauthorized release of sensitive and/or confidential information, and unauthorized disclosure of trade secrets, copyrights, and other intellectual property that might be stored on the hard disks and other storage media. It should be noted that all agencies computer hard drives especially those containing sensitive and/or confidential data must have all Colorado data securely removed from their hard drives as specified by this policy before a computer system is surplused, transferred, traded-in, otherwise disposed of, or the hard drive is replaced.

Removal of confidential information in the past might have been accomplished by using the FORMAT command or the DOS FDISK command. Ordinarily, using these procedures gave users a sense of confidence that their data had been completely removed. When using the FORMAT command, Windows displays a message such as:

Important: Formatting a disk removes all information from the disk.

The FORMAT utility actually creates new FAT or ROOTS tables, leaving all previous data on the disk untouched. Moreover, an image of the replaced FAT and ROOT tables are stored, so that the UNFORMAT command can be used to restore them. FDISK merely cleans the PARTITION TABLE (located in the drive's first sector) and does not remove anything else.

In recent years advances in data recovery have been made such that data can be reclaimed in many cases from hard drives that have been wiped or cleared. Free and commercial software exist that use techniques such as Partial Response Maximum Likelihood (PRML) and Magnetic Force Microscopy (MFM) and other recovery methods based on patterns in erased bands to recover cleared data.

Therefore, the Colorado Information Security Task Force (CISTF) has determined the State standard herein to eliminate or reduce information security risks to the greatest extent possible. The intent of this standard is to introduce and follow a zero-liability model for information security upon the surplusing, transfer, trade-in, disposal of computers, or replacement of computers and other electronic storage media, and computer software.

Approach

The heads of State agencies, the heads of their field offices, and the heads of institutions of higher education are responsible for compliance with this standard.

Failure to expunge data that might be exposed under risk situations could violate federal laws including but not limited to the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act of 1996 (HIPPAA), The Family Education Rights and Privacy Act (FERPA), etc.

This standard applies to equipment owned or leased by the agency. All hard drives (this includes instances where equipment has multiple hard drives) and electronic storage media shall have all Colorado data properly removed prior to disposal or release. Data removal procedures shall be properly documented in accordance with the processes outlined below in sections B, C and D to prevent unauthorized release of sensitive and/or confidential information that may be stored on that equipment and other electronic media. This is to include all computer equipment that has memory such as personal computers, PDAs, cell phones, pagers, routers, firewalls and switches.

Examples of other media include, but are not limited to, tapes, diskettes, CDs, DVD, worm devices, and USB data storage devices.

Reviews

A full review of this Colorado Information Technology Resource Management Standard for the Removal of Colorado Data from Surplus or End of Life Computer Hard Drives and Other Electronic Media is anticipated annually.

CISTF Requirements for Electronic Data Destruction

This section groups the specifications of the removal of Colorado data from Computers and other Electronic Media.

A.Data Destruction

All agencies as well as their field offices must follow the following standards when a computer system is surplused, transferred, traded-in, or disposed of, or the hard drive is replaced. The following standards apply to owned, leased or contractor-supplied computers.

A.1 General Standards

A.1.a Before a computer system is surplused, transferred, traded-in, disposed of, or the hard drive is replaced, all sensitive and/or confidential program or data files on any storage media must be completely removed or otherwise made unrecoverable in accordance with this procedure unless there is specific intent to transfer the particular software or data to the purchaser/recipient.

A.1.b Hard drives or other electronic storage media of surplus computer equipment must be securely erased according to this procedure within 60 days after disposition decision is made, and always prior to release outside the agency.

A.1.c Whenever licensed software is resident on any computer media being surplused, transferred, traded-in, disposed of, or the hard drive is replaced, the terms of the license agreement must be followed. In most cases, the software must be totally removed from the computer media.

A.1.d After the removal of Colorado data from the hard drive or other electronic media is complete, the process must be certified, as specified in this standard, and a record maintained as specified by the agency's records retention schedule.

A.1.e Each agency head or head of an institution of higher education should randomly test for compliance with this standard any computer hard drives or electronic media that are surplused, ready for public auction, transferred, traded-in, disposed of, or when the hard drive is being replaced.

B.Colorado End-of-Life Computers and Other Electronic Devices/Media Standards

The following section outlines the acceptable methods to expunge data from hard drives, other electronic devices and storage media. Colorado data destruction must be performed to ensure that information is removed in a matter that gives assurance that the information cannot be recovered.

The method used for removal of Colorado data, depends upon both upon the operability of the hard drive, the classification of data (the nature of the data residing on the hard drive), and the age of equipment.

- Operable hard drives that will be reused must be sanitized prior to disposition according to this standard. If the operable hard drive is to be removed from service completely, **it should be physically destroyed**. The destruction process must comply with all state and federal environmental laws. If the hard drive will be reused outside of the originating agency, it must be either overwritten or degaussed according to this standard.

- If the hard drive is inoperable or has reached the end of its useful life, **it should be physically destroyed**.

- Other media, including, but not limited to tapes, diskettes, CDs, DVDs, worm devices, and USB data storage devices; and all other electronic devices that has a memory such as personal computers, PDAs, cell phones,

pagers, routers, firewalls and switches that hold user data or configurations in non-volatile memory shall have all Colorado data removed by:

* If there is any risk of disclosure of sensitive data, **it must be physically destroyed**.
* Removal of the battery or electricity supporting the non-volatile memory
* By such other method recommended by the manufacturer for devices

- If data on the hard drive or other electronic media or device is deemed to fall within the scope of applicable state and federal security, and/or privacy laws, **it should be physically destroyed**. The Executive Director of the agency, or his/her designee shall make determination of the data with respect to applicable state and federal security, and/or privacy laws. Guidelines for such classifications follow:

Guidelines for data and computer equipment classification:

Data
"Treat your data as you would an investment. Would a "prudent man" entrust his investments to convicted felons? Is the data sensitive enough that someone who recovers it could commit identity theft (name associated with social security number)? Is there payroll or other private employee information on it? Is there individually identifiable medical information on it? Ultimately, Colorado agencies are responsible for data security and sanitization. Agencies have a fiduciary responsibility to protect critical data. Failure to fulfill that responsibility can expose Colorado to legal liability and, in some cases, criminal prosecution. Colorado can outsource the task, but cannot outsource the responsibility for improper data disposal or access." – paraphrased from Gartner Research 2002 TG-15-6943, 2 April 2002.

Computer/Equipment
"The value of PC equipment is limited. Equipment that is less than 24 months old has some value and can possibly be redeployed or resold. Equipment beyond three years old, however, generally has value only as spare parts. Therefore, for older equipment, Colorado should investigate whether the cost associated with the secure sanitization of hard drives will exceed the proceeds from selling the equipment and, if so, they should look at total destruction as the primary option for data sanitization." "Shielding Colorado from risk (vs. capturing economic opportunity) must drive rational data sanitization policies for the disposal of surplus or obsolete IT equipment." – paraphrased from Gartner Research 2002 TU-15-8513, 2 April 2002.

Acceptable methods to remove data:

Before the removal process begins, the computer **must be disconnected from any and all networks** to prevent accidental damage to the network operating system or other files on the network. If the data resident on an operable hard drive is needed on another device, remember to back up data before sanitizing hard drives.

There are three acceptable methods to be used for the hard drives, all in compliance with the Department of Defense (DOD) Standard 5220.22-M:

- Physical Destruction
- Degaussing
- Overwriting

Physical Destruction

Total physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive. Total destruction means just that — to destroy the hard drives and the platters within. It is the absolutely only way to guarantee all data on the hard drive is destroyed and therefore irrecoverable.

B.1 Physical Destruction Standards

B.1.a Hard drives must be destroyed when they are defective or cannot be economically repaired or Colorado data falls within the scope of applicable agency determination of security risk, Information Security Task Force determination, or cannot otherwise be reasonably removed for reuse.

B.1.b Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive. Total destruction is defined as "to disintegrate, incinerate, pulverize, shred or melt the hard drive." At the end of the process, the hard drive should be destroyed to the extent that it cannot be reinserted into a functioning computer.

B.1.c All destruction vendors must comply with all state and federal security, privacy, environmental, and hazardous waste laws. Specific language must be incorporated in all PO's, contracts, and/or in State Price Agreement vendor relationships to ensure compliance.

Degaussing

Degaussing is a process whereby the magnetic media is erased. Hard drives may become inoperable after degaussing. The degaussing method will only be used when the hard drive is inoperable or when the hard drive will not be used for further service.

Please note that extreme care should be used when using degaussers since this equipment can cause extreme damage to nearby telephones, monitors, and other electronic equipment. Also, the use of a deguasser does not guarantee that all data on the hard drive will be destroyed. Degaussing efforts will be audited periodically to detect equipment or procedure failures. The following standards must be followed when hard drives are degaussed:

B.2 Degaussing Standards

B.2.a Follow the product manufacturer's directions carefully. It is essential to determine the appropriate rate of coercivity for degaussing.

B.2.b Shielding materials (cabinets, mounting brackets), which may interfere with the degausser's magnetic field, must be removed from the hard drive before degaussing.

B.2.c Hard disk platters must be in a horizontal direction during the degaussing process.

Overwriting

Overwriting is an approved method for the removal of Colorado data from hard disk drives. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable without specialized equipment. Overwriting can be used to surplus or externally reuse operable hard drives. All software products and applications used for the overwriting process must meet the following standards:

B.3 Overwriting Standards

B.3.a The data must be properly overwritten with a pattern. Department of Defense (DOD standard 5220.22-M) requires overwriting with a pattern, and then its complement, and finally with a random pattern of 1's and O's.

B.3.b Removal of Colorado data is not complete until it meets the DOD standard 5220.22-M which is currently at least three overwrite passes and a verification pass is completed.

B.3.c The software must have the capability to overwrite the entire hard disk drive, independent of a BIOS or firmware capacity limitation that the system may have, making it impossible to recover any meaningful data.

B.3.d The software must have the capability to overwrite using a minimum of three cycles of data patterns on all sectors, blocks, tracks, and any unused disk space on the entire hard disk medium.

B.3.e The software must have a method to verify that all data has been removed. Recommended software packages are listed at the end of this document.

Unacceptable methods to remove data:

Clearing data (deleting files) is NOT ACCEPTABLE: Clearing data (deleting files) removes information from storage media in a manner that renders it unreadable unless utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by technical means, it is **not** an acceptable method of removing Colorado data from agency owned hard disk storage media. The only exception to this is when computers are being redeployed internally within the agency.

C.Certification of Total Destruction (Data and Physical)

Each agency is responsible to:

- Obtain a certification of total destruction for each device destroyed, and
- Audit the removal of Colorado data for compliance with this standard when any computer hard drives or electronic media are surplused, transferred, traded-in, disposed of, or the hard drive is being replaced as well as to insure the audit process occurs in a timely manner, and the audit controls are effective.

D.1 Standards

D.1.a Prior to submitting surplus forms to the agency's appropriate organizational unit, the process for removal of the Colorado data must be documented on a form that explicitly outlines:

1. The method(s) and rationale used to destroy the device or to expunge the data from the storage media.
2. The serial number or other tracking number on a log centrally located and maintained.
3. The type of equipment/media being destroyed or from which Colorado data is removed.
4. The name of the person responsible for the destruction decision and the vendor or for the removal of Colorado data.
5. The final disposition and date of disposition.

D.1.b For destroyed items, the completed forms must be maintained in a central location for audit purposes. For refurbished, redeployed, surplused, or otherwise reused items, the form must be completed and a copy affixed to the hard drive. Additionally, the completed forms must be maintained in a central location for audit purposes.

D.Exceptions and Clarifications to Policy/Standards

E.1 Exceptions

E.1.a CPU's may be surplussed only when the hard drive has been completely removed. CPU's include the metal casings, motherboards, circuitry, or any other component that may have volatile memory. However, any flash memory like those used in IPAQ and Palm devices that do retain data IS included, and therefore is not an exception.

E.1.b Inoperable equipment (excluding monitors) that may be economically repaired does not have to be destroyed. Inoperable equipment must be destroyed according to this standard and the Colorado Department of Public Health and Environment (CDPHE)'s policy for electronic waste (http://www.cdphe.state.co.us/hm/electronics.pdf).

E.2 Clarifications

E.2.a If any equipment named in this standard does not meet the criteria herein (operable, does not contain data or software security risks as determined by the agency executive director or designee), agencies should follow the overwriting standard, remove proprietary software and follow the normal surplus process.

E.2.b Inoperable equipment (excluding monitors) that may be economically repaired does not have to be destroyed. Agencies may repair, re-use or follow the overwriting standard, remove proprietary software and follow the normal surplus process.

E.2.c State Surplus may continue to receive operable monitors, keyboards, CPU's (minus the hard drives), hard drives that have been determined to not have confidential information AND agencies will not be internally redeploying AND due diligence was performed (overwriting), and other peripherals (such as the mouse).

E.2.d State Surplus may not participate in the destruction of hard drives or other non-volatile storage devices.

E.2.e Inoperable or end-of-life equipment where the unit is under warranty or is leased must follow the same process, in terms of vendor certification of data destruction and hardware disposition, maintaining the security of all data and intellectual property, providing a high degree of security in the pick-up, transportation, storage and processing, compliance with state and federal security, privacy laws and regulations, ensuring that nothing is dumped into landfills, and providing a complete audit trail and certification of the destruction of the data and non-vendor related software.

E.Standards for Data and Physical Destruction Vendors:

ALL Vendors Must:

- Comply with state and federal security, privacy environmental, and hazardous waste laws and regulations.
- Maintain the security of all data and intellectual property.
- Disassemble old computer hardware and then re-process all materials (glass, plastic and metal) for re-use
- Ensure that nothing is dumped into landfills.
- Destroy hardware, software and data from electronics if not already done.
- Provide a high degree of security in the pick-up, transportation, storage and processing of computer equipment
- Provide a complete audit trail and certification of the destruction of the data, software and hardware.
- Meet all other State contract requirements
- PLEASE REFER TO LIST OF QUESTIONS FOR POSSIBLE VENDORS during the pilot. Once statewide price agreements are in effect, compliance with state and federal security, privacy, environmental, and hazardous waste laws will be incorporated into the contracts.

Vendors MUST NOT:

- Donate old computer hardware/equipment.
- Dump any portion of old computer hardware/equipment in landfills.
- Refurbish and/or re-sell old computers (State Surplus excepted).
- Ship old computers overseas.
- Sell anything from old computers collected (State Surplus excepted).

F.Possible tools:

According to the manufacturer's claims, the following software meets Department of Defense (DOD) Standard (5220.22-M) for the removal of data from hard drives and are, as examples, suggested for use:

- Active@KillDisk by L Soft Technologies, Inc. (Free)
- Wiperaser XP by LIVeye, SDC (Shareware)
- Eraser by Heidi Computers, LTD (Free

- GDISK by Symantex, Inc.
- BC-WIPE (shareware) – can be downloaded from www.jetico.com

BC-WIPE by Tucows, Inc.